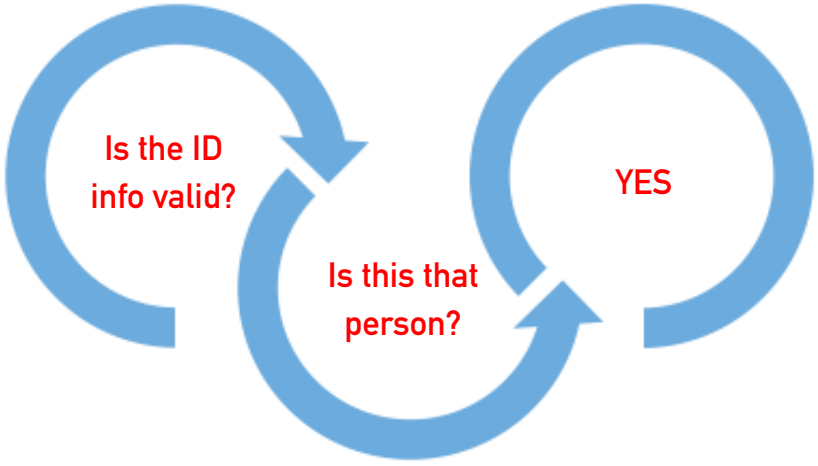
Validate, Authenticate & Determine Customers' Propensity to Pay

Leverage New Models to Simplify Banking Authentication

Presented by Secure Identity Systems

In an often "customer-not-present" world, financial institutions need adaptive tools that meet organizational policies and integrate easily into existing platforms to mitigate fraud and data inconsistencies.



Most financial institution's needs are twofold.

1. Validate & Authenticate: Validate that an ID is in fact a valid form of ID and authenticate that the person using the ID is in fact the person on the ID.
2. Account Risk Verification: Determine the individual's "propensity to pay."

Financial institutions need to do all this remotely, while achieving a virtually instant response. It sounds difficult, and it is, but this white paper will break down this mythical feat into two easy-to-understand and implement steps.

1. Validate & Authenticate

Identity validation enables financial institutions to establish and maintain secure relationships with their customers by quickly validating consumer-supplied identifying information. Your identity validation product should deliver above-average hit rates on validation inquiries to under-banked populations and individuals with little to no credit history as well as accurate fraud detection.

Identity authentication presents your customer a series of customizable, multiple choice, non-credit based questions that are easily answered by a legitimate customer. Answers are scored based on accuracy matches. Identity authentication supports regulatory compliance.

Automatic Data Population
Automatic Data Population is an added-value feature that replaces manual input and assists financial institutions in obtaining and identifying information while opening accounts quickly and efficiently with fewer human errors.

With the swipe of a valid Driver's License — or any ID with a barcode or magnetic stripe — fields are populated with all the necessary information to open an account and create a digital file of the license that automatically populates into your core system. The same data can then be repopulated into other system field forms, eliminating the need to retype customer's information and solving the problem of input errors as well as saving time.

In addition to operational benefits, compliance benefits include:
Online "selfie" submission capabilities for ID match verification
Flexibility to customize the account opening fields to reflect policies and procedures
The ability to mandate fields and require completion for account opening staff

2. Account Risk Verification

Account Risk Verification (ARV) uses a bank account and routing number to access a person's real-time account info that includes the last 90-days of account history. It's an inexpensive model that uses deep reaching information to assess risk and propensity to pay.

ARV Information includes:
Verified ABA numbers
Accept/Decline/Warning/Unable to Verify responses
Up to two first and last names associated with the magnetic ink character recognition (MICR)
Ability to match name provided and name associated with MICR
Up to two phone numbers associated with MICR
Number and dollar amount of all paid and unpaid returned items, with average number of days to repay

ARV+ Code Model
In addition to looking at current account history, bank information, collection history and bill payment patterns, the ARV+ Code model alerts financial institutions when an account has had an associated unauthorized return or returns for account data quality issues in the last 12 months. This is particularly important due to the new NACHA regulations that restrict unauthorized returns to 0.5%, and a 3.0% cap on returns for data quality issues.

NACHA's Rule to Address Excessive Transaction Return Levels Goes into Effect

In September 2015, the new ACH Network Risk and Enforcement Rule went into effect. The rule lowers the existing return threshold for unauthorized transactions from 1.0% to 0.5%, and expands NACHA's authority to enforce the rules related to unauthorized transactions. The rule also establishes an inquiry process that can be used when an originator or third-party sender exceeds an administrative return rate level of 3.0% and/or an overall return rate level of 15.0%. While exceeding these new return rate levels is not automatically considered a violation of the NACHA rules, originators and third-parties can be required to reduce their return rates when an inquiry shows that poor origination practices have resulted in excessive returns. (Source: NACHA.org)

About Secure Identity Systems
Secure Identity Systems was initially created to mitigate the risk for financial institutions by identifying growing security threats. By 2006, Secure Identity Systems held three North American Patent Rights for ID Theft prevention and authentication. By the time the regulatory "Joint Release Red Flag Rule" was handed down, SIS was the only company in the U.S. to have a complete end-to-end solution already in place. Today, SIS serves financial institutions, businesses and families with the most robust products and services available.

For more information on Secure Identity Systems, please call 877.304.3349 or visit SecureIdentitySystems.com. Follow Secure Identity System on Facebook and Twitter for security updates and special offers.